WHAT IS CLAIMED IS:

1. A method of generating a CRC for a composite sub-message based on a CRC generating polynomial having at least two factors, the composite sub-message including sub-message data and a number, n, of trailing zeros, the method comprising:

generating a first remainder based on the sub-message data and a first factor of the CRC generating polynomial;

generating a second remainder based on the sub-message data and a second factor of the CRC generating polynomial; and

generating the CRC for the composite sub-message based on adjusted versions of the first and the second remainders.

2. The method of claim 1, and further comprising:

adjusting at least one of the first and the second remainders based on the number, n, of trailing zeros in the composite sub-message.

3. The method of claim 2, wherein the first remainder is an m-bit remainder, and wherein the adjusting step comprises:

storing the first remainder in an m-bit memory location;

examining each bit of N, where N equals n mod $(2^m - 1)$; and

selectively advancing the contents of the m-bit memory location to a next state based on a value of each bit of N, the next state determined by a Galois field defined by the first factor.

4. The method of claim 3, wherein the second remainder is adjusted in substantially the same manner as the first remainder.

5. The method of claim 2, wherein the first remainder is an m-bit remainder, and wherein the adjusting step comprises:

storing the first remainder in an m-bit memory location; and

examining each bit of N, where N equals n mod $(2^m - 1)$, in order from a most significant bit to a least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to a next state as determined by a Galois field defined by the first factor.

6. The method of claim 5, wherein the second remainder is adjusted in substantially the same manner as the first remainder.

7. The method of claim 1, wherein the step of generating a first remainder comprises:

dividing the sub-message data by the first factor.

8. The method of claim 7, wherein the step of generating a second remainder comprises:

dividing the sub-message data by the second factor.

9. The method of claim 1, wherein the step of generating a first remainder comprises:

dividing the sub-message data by the CRC generating polynomial, thereby generating an unadjusted composite remainder; and

dividing the unadjusted composite remainder by the first factor, thereby generating the first remainder.

10. The method of claim 9, wherein the step of generating a second remainder comprises:

dividing the unadjusted composite remainder by the second factor, thereby generating the second remainder.

11. The method of claim 1, wherein the step of generating the CRC comprises mapping the adjusted versions of the first and the second remainders to a corresponding CRC.

12. The method of claim 11, wherein the mapping is performed with a fixed logic circuit.

13. The method of claim 1, wherein the first and the second factors are primitive polynomials.

14. The method of claim 1, wherein the first and the second factors are irreducible polynomials.

15. A method of generating a CRC for a composite sub-message based on a CRC generating polynomial having at least two factors, the composite sub-message including sub-message data and a number, n, of trailing zeros, the method comprising:

generating an unadjusted composite remainder representing a remainder of a division of the sub-message data by the CRC generating polynomial;

generating a first factor remainder representing a remainder of a division of the unadjusted composite remainder by a first factor of the CRC generating polynomial;

generating a second factor remainder representing a remainder of a division of the unadjusted composite remainder by a second factor of the CRC generating polynomial; and

generating the CRC for the composite sub-message based on adjusted versions of the first factor remainder and the second factor remainder.

16. The method of claim 15, and further comprising:

generating the adjusted version of the first factor remainder based on the number, n, of trailing zeros in the composite sub-message using finite field squaring and advancing states in a Galois field defined by the first factor.

17. The method of claim 15, wherein the second factor is x + 1, the method further comprising:

generating the adjusted version of the second factor remainder based on a parity computation of the unadjusted composite remainder.

18. The method of claim 15, wherein the second factor is x + 1, and wherein the CRC generating polynomial has an order of R, and wherein the step of generating a first factor remainder comprises:

testing a most significant bit of the unadjusted composite remainder;

setting the first factor remainder equal to the R-1 least significant bits of the unadjusted composite remainder if the tested bit is equal to zero; and

setting the first factor remainder equal to the R-1 least significant bits of a result of an XOR of the unadjusted composite remainder and the first factor if the tested bit is equal to one.

19. A method of generating a CRC for a composite sub-message based on a CRC generating polynomial having at least two factors, the composite sub-message including sub-message data and a number, n, of trailing zeros, the method comprising:

generating a first factor remainder representing a remainder of a division of the sub-message data by a first factor of the CRC generating polynomial;

generating a second factor remainder representing a remainder of a division of the sub-message data by a second factor of the CRC generating polynomial; and

generating the CRC for the composite sub-message based on adjusted versions of the first factor remainder and the second factor remainder.

20. The method of claim 19, and further comprising:

adjusting at least one of the first factor remainder and the second factor remainder based on the number, n, of trailing zeros in the composite sub-message using finite field squaring and advancing states in at least one Galois field defined by at least one of the first and the second factors.